Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERT-FR

Paris, le 05 septembre 2014
N° CERTFR-2014-ACT-036

Affaire suivie par :
CERT-FR

BULLETIN D'ACTUALITÉ

Objet : Bulletin d'actualité CERTFR-2014-ACT-036

1 - Publication du guide de recommandations de sécurité relatives à Active Directory

L'ANSSI publie un guide de recommandations de sécurité relatives à Active Directory. Ce guide s'adresse à toute organisation utilisant un domaine Windows géré par Active Directory.

Active Directory est un annuaire permettant de centraliser les informations relatives aux utilisateurs et aux ressources d'une entité. Cet annuaire fournit des mécanismes d'identification et d'authentification tout en sécurisant l'accès aux données. Celui-ci occupe généralement un rôle central dans le système d'information de l'entreprise et en devient donc un élément critique. En effet, l'obtention à des fins malveillantes d'un compte privilégié au sein d'Active Directory peut entraîner la compromission des secrets utilisateur, des données métier ainsi que des postes de travail et serveurs de l'infrastructure.

Ce guide a pour but de présenter :

- les concepts relatifs à Active Directory ;
- les bonnes pratiques en matière de configuration, d'architecture et d'administration ;
- les éléments importants à contrôler au quotidien.

Le CERT-FR recommande aux entités possédant un domaine Active Directory de contrôler les différents éléments décrits et de mettre en œuvre les préconisations de ce guide.

Documentation

- Guide sur les recommandations de sécurité relatives à Active Directory :
  http://www.ssi.gouv.fr/IMG/pdf/NP_ActiveDirectory_NoteTech.pdf

2 - Conservation des en-têtes d'un message électronique dans le cadre de l'investigation numérique

Le CERT-FR est fréquemment amené, dans le cadre de ses missions, à analyser des messages suspects transmis par des administrations ou des partenaires afin d'en déterminer la malveillance.

Afin de préserver au mieux les traces d'un message, il convient de :

- ne pas transférer ni copier-coller le contenu du message malveillant : cela supprime les en-têtes qui contiennent des informations utiles telles que l'adresse des serveurs relais, l'expéditeur et les conditions dans lesquelles le message a été traité par le serveur SMTP ;
- transmettre le message compressé avec un utilitaire tel que 7-zip à l'aide d'un mot de passe : cela permet la transmission des messages sans altération et empêche l'activation par erreur de l'éventuelle charge malveillante.

Dans le cadre de l'analyse, les en-têtes peuvent être affichés de la manière suivante :

- avec le logiciel Microsoft Outlook : ouvrir le message et sélectionner «Propriétés» dans le menu fichier ;
- avec le logiciel Mozilla Thunderbird : sélectionner le message sans l'ouvrir dans la liste des messages reçus, puis appuyer sur les touches `Ctrl+U` afin d'afficher la source du message ;
- avec le logiciel Lotus Note : ouvrir le message et sélectionner «afficher la source» dans le menu affichage.

Documentation

- Mesures de prévention relatives à la messagerie :
  http://www.cert.ssi.gouv.fr/site/CERTA-2000-INF-002/index.html
- http://www.signal-spam.fr/plugins/trouver-len-tête-dun-mail-sous-thunderbird-15
- http://www.office.microsoft.com/fr-fr/outlook-help/afficher-les-informations-den-tete-internet-des-messages-electroniques-HA101836448.aspx

3 - Rappel des avis émis

Dans la période du 29 août au 04 septembre 2014, le CERT-FR a émis les publications suivantes :

- CERTFR-2014-AVI-368 : Vulnérabilité dans IBM Tivoli
- CERTFR-2014-AVI-369 : Vulnérabilité dans Squid
- CERTFR-2014-AVI-370 : Vulnérabilité dans Citrix CloudPlatform
- CERTFR-2014-AVI-371 : Multiples vulnérabilités dans phpMyAdmin
- CERTFR-2014-AVI-372 : Multiples vulnérabilités dans les produits Mozilla
- CERTFR-2014-AVI-373 : Multiples vulnérabilités dans le noyau Linux d'Ubuntu

Gestion détaillée du document

05 septembre 2014 version initiale.